OPERATIONAL RISK MANAGEMENT FOR THE UNITED STATES MANNED SPACE FLIGHT PROGRAM

PREPARED FOR THE SOCIETY FOR RISK ANALYSIS

CHARLES S. HARLAN
NASA JOHNSON SPACE CENTER
OCTOBER 1985

OPERATIONAL RISK MANAGEMENT
THE UNITED STATES MANNED SPACE FLIGHT PROGRAM

OPERATIONAL RISK MANAGEMENT FOR MANNED SPACEFLIGHT

This paper provides an overview of the risk management appraoch taken for the National Space Transportation System Program with background discussion from previous manned space projects. The National Space Transportation System Program is the current operating manned space program and is also known as the Space Shuttle Program. the process for risk management is discussed, with emphasis on the management approach throughout the life cycle of the program. In any dynamic, highly visible program of major significance, risk assessment must be a continuing process with broad participation of all the disciplines involved in the program.

INTRODUCTION

The Space Shuttle is the mainstay of the National Space Transportation Systems Program. As such, it represents the total capability of the United States for launching men and women into near-earth orbit. Additionally, it represents a significant fraction of the current operational U.S. capability to launch unmanned spacecraft into space. it was decided early in the program that the Space Shuttle would be the primary transportation system for both civilian and military payloads.

As of this writing, twenty successful Space Shuttle missions have been flown indicating a sound concept and a clear trend towards the final development of an operational program. The risk management approach for the space Shuttle has evolved from a legacy of previous manned programs, indicating a sound and workable approach to dealing with the class of risks associated with the complex and hazardous technology involved. The approach and methodology to program risk management have changed with time as technology has changed, and will have to continue evolution if the same degree of success is to be achieved in the future.

Four to seven crew members and the spacecraft are typically exposed to mission risks for durations of a week to ten days on Space Shuttle Missions. The flight duration, crew compliment, and payloads are functions of the individual mission requirements. Onorbit risk exposure is determined by mission requirements, and risks associated with launch and reentry are present for each flight. The payloads are often sophisticated state-of-the-art devices requiring special services from both the Orbiter systems and the crew. The payloads and experiments require individual analysis and consideration for the risks that are potentially present to the Space Shuttle and the crew.

Considering the importance that the Space Shuttle has to the Nation and the fact that human lives are involved in every flight, risk management is a high priority activity throughout the entire life cycle of the program. While the program is continually moving towards a fully operational state, the emphasis on risk management must not be abated because of continuing change in flight content and the reality that a quasi-operational phase will exist until design, technology, and operational methods are fully understood and determined to be acceptable for routine flight.

The current analytical techniques used to assess risks in the manned programs have evolved to their present state of utility over a number of years. These techniques have not kept up with the complex technology involved in the flight and ground systems being contemplated, especially when considering the widespread application of computer-controlled logic intermixed with dynamic hardware systems. New methods of analysis and risk assessment must be developed to deal with complexities of evolving technologies in tomorrow's flight programs.

MANNED SPACE FLIGHT BACKGROUND

Aerospace programs, both manned and unmanned, began to develop comprehensive risk assessment and managment tecniques some 25 years ago. Weapons systems, as well as systems being considered for manned flight, were becoming much more complex and costly as mission demands were increasing. addition of a flight crew brought yet another concern regarding the degree of potential risk acceptable when human life is involved. The extreme visibility given to the manned element of NASA's program, well in advance of the first flight, added to the level of concern in the overall program risk analysis equation.

The field of systems engineering and systems safety engineering naturally grew out of the demands of these factors. Investigations of the many early accidents and test failures led to design errors, lack of quality control, manufacturing defects, or other problems associated with the concept, design, fabrication, and operation of the system. all of these factors had to be considered in the analysis and determination or risk acceptability. The manned space program derived its engineering, management, and operationl methodology from the aircraft development programs and the early missile systems development programs.

SPACE SHUTTLE PROGRAM RISK MANAGEMENT APPROACH

The Space shuttle Program is comprised of a number of major projects called program elements. The program elements are the Orbiter, the external Tank, the Shuttle Main Engines, the Solid Rocket Boosters, and the Launch and landing facilities. These projects are managed by Project Offices located in different geographical locations in the NASA system. The overall Program policy and direction comes from the Level I Program Office at NASA Headquarters in Washington, D.C. The overall technical integration and direction to the element Project Offices come from the Level II Program Office

located at the Johnson Space center in Houston, Texas. The element project offices, sometimes referred to as Level III, are responsible for the management of the separate elements of the Program and work through the Level II Office for integration with the other elements.

With this hierarchical structure in place for the total management of the Program, the responsibility for risk assessment and management is shared by all three levels. In that regard, formal managmeent control mechanisms have been established at each level to insure that the proper degree of responsiveness i meeting requirements and issues is appropriately addressed. Overriding this whole programmatic structure are formally-constituted program oversight groups and periodic top management reviews which are established either on a flight-by-flight basis or to deal with specific concerns.

The management approach for the Space shuttle Program is an outgrowth of the Apollo program; however, there is increased emphasis in the area of project integration. For the Apollo and previous manned programs the essential functions of Level I and Level II were combined in the NASA Headquarters Program Office. The addition of the Level II Program Office to the management scheme added a significant capability to review and control the requirements associated with risk decisions. It is a focal point where the significant technical issues from the total Program come together. All risk situations have an effect on the total program; therefore, it is natural that the focus for risk decisions centers at the Level II Program Office with participation from NASA Headquarters as required in the resolution of the major issues. The management review process involving both the Level I and II Offices is largely a joint activity utilizing common data provided by the Level II Integration Office and/or the Level III Project Offices.

The management decisions at the different levels are made by key managers associated with all other major project decisions. The same decision forums (typically Configuration and Requirements Control Boards) used for the other important decisions are used indetermining the acceptability of potential risks. Ultimately, the acceptance of any degree of risk is a program management decision because of the many factors involved that can only be considered and traded off at the top program level. On the other hand, there has to be a process and an organization charged with the responsibility of understanding the risks in a program and to bring information regarding these risks into the decision-making process. In most aerospace organizations this responsibility normally belongs to some form of product assurance function - typically the Safety and Reliability disciplines.

In the Space shuttle Program the forum used for review and assessment of risks by the Level II Program Office is the program Requirements Control Board (PRCB). The PRCB involves all Program functional disciplines and element Project Offices. The fact that all of these entitites are required to participate in regular reviews of risk issues provides program-wide incentive to give high priority to the subject.

The safety organizations in the various areas are responsible for doing the basic staff work to bring these issues to the decision forum. The safety organization at the Level II or Program Integration Level is responsible for the formal integration of the risk assessment activity across the whole program. The Flight and Ground Operations Organizations also provide an independent systematic engineering review on a flight-by-flight basis as a by-product of their normal mission preparation work. Both of these thrusts are important inputs to the risk management decision process since they are regular ongoing functions throughout the life of the program.

The management forum dealing with the closeout of issues relating to risk for each flight is called the flight readiness review (FRR). The Space Shuttle Flight readiness Review Board is chaired by the Level I Program Director; and each problem, failure, or potential risk issue which occurred during or since the previous flight is discussed and resolved. this forum has high visibility and is mandatory event prior to each flight.

The FRR Board is comprised of essentially the same management team that has dealt with program risks to date, thus providing essential program continuity. The main difference is the emphasis, as there will be no affirmative decision for flight unless all risk decision criteria are met. This puts extreme pressure on all Program elements to deal with these issues early on. Anyone having a valid concern relating to the flight in question can raise it before this group and have it considered prior to flight. By using this technique, the management assessment of total or aggregate program risk is continually kept up to date as it related to the currently planned flight. The product assurance organizations have the responsibility to insure that all open concerns are discussed during the FRR's, and to give a formal accounting of their status for each flight.

Aside from the comprehensive attention given the subject by different levels of Agency management, there are external oversight groups which assess NASA's adequacy in dealing with program risks. Some are appointed on an Ad Hoc basis to deal with specific issues and may be appointed by the Administrator to assess a particular problem area. There is one standing committee made up of senior officials in the aerospace industry called the Aerospace Safety Advisory Panel (ASAP), that is chartered by the congress. The ASAP is charged with conducting an annual assessment and reporting to Congress on NASA's performance in dealing with manned program risks. This has

been a long standing committee since the early days of the Apollo Program which has free access to information and people (including the contractors) associated with the risk process.

There are a number of analysis techniques performed by the Safety and Reliability organizations at the various program levels which are used to formally provide the risk baseline inputs for management review of both the flight and ground systems. These techniques are typical of those found in most aerospace development programs and represent the basic capabilities available today for this type of engineering. At this point they are strongly biased towards hardware systems because cost-effective hazard analysis techniques for other areas are unavailable.

There are a number of processes routinely used in the Space Shuttle Program that are not optimized to support risk management per se, yet they are effective when considered on a total Program basis because of their capability to meet other priority needs as well. there has been a heavy emphasis on testing, simulation, and various empirical techniques to support the development process. Because of the high cost of this process, the number of cases or conditions considered is always restricted thereby limiting the total scope of the hazard analysis. For this reason, testing, simulations, and actual flight operations involving the completed system in a ready-to-fly configuration have yielded many surprises relative to the discovery of new hazards. Not surprisingly, there is still a heavy commitment on these processes to accept systems for flight.

The determination that software is acceptable for flight from a risk standpoint is accomplished for each build of flight and ground software, and involves a rigorous series of tests commencing with the individual software modules and ending with full scale verification testing of actual flight-type

hardware. The full scale verification testing is done in a sophisticated laboratory (Shuttle avionics Integration Laboratory) involving real flight hardware, real flight cabling, and typical cockpit inputs for the situation being tested.

The total body of testing and analysis to assess risks and to provide information for the control and elimination of risks has been structured for the Space Shuttle Program to make the best use of available techniques and resources to accomplish the total program task. As new programs such as the Space station develop, a different mix of analyses based on similar rationale will be used; however, the available analytical techniques will have progressed significantly to allow a more thorough and cost-effective approach to support the risk management process.

Program risks that are neither controlled nor eliminated must be considered acceptable to Program Management based on sound engineering rationale. An example of an acceptable risk would concern the structural integrity of a main engine 17-inch propellant feed line. While adding a redundant line might keep the engine running in the event of a ruptured line, the result of the first failure during flight would be a catastrophic loss of the Orbiter and crew. this risk is acceptable to the Program for a variety of reasons involving the use of approved design factors, proof-of-design efforts, qualification testing, manufacturing, product inspection, and constraining flight conditions to be within allowable limits. While there are some accepted risks such as the structural example used here that cannot be eliminated, there are others that can be eliminated over time.

At any point in a program, there will always be some degree of risk that can be eliminated with additional development effort. This of course requires time and resources, and the major question becomes whether the currently-understood aggregate risk is acceptable until some reduction is made. The total number of accepted risks baselined for the first Space Shuttle flight was 138. The number of accepted risks for the most recent flight has been reduced to 98. This is a whopping 29-percent reduction, made possible by an aggressive program-wide effort to continue finding ways to minimize Program risks.

As previously mentioned, the operations organizations provide a significant contribution to the risk management process. The operations oragnaization has to live with all known and unknown risks associated with the system at the time of flight. It is NASA practice to have involvement of engineers from the operations organization in all phases of the manned space flight program from initial concept definition throughout the entire life cycle. This involvement constitutes a significant "systems engineering" capability focused on a systematic evaluation of the systems, procedures, and operations plans. it is particularly useful isnce it comes from the viewpoint of how the end user will have to cope with the system should these risk scenarios develop in flight. It is an entirely different view of the system than a design or assurance organization would have, and results in an output that complements the total risk management process.

Many of the residual hazards not eliminated during the desing and development process have to be controlled by crew action, should the situation arise. The controls frequently require the use of complex procedures or a long sequence of complex procedures involving either the crew, the ground controllers, or both. Often sophisticated warining systems are required along

with ground support capabilities that use telemetry and tracking data to evaluate flight progress. Inflight failures often result in conditions of sigmificant risk to the crew and spacecraft in very short periods of time. Preplanned actions and detailed procedures are necessary to cope with these situations.

The operations team must be able to maintain a high degree of proficiency to properly respond to this type of contingency. This requires a significant investment in training and the conduct of high fidelity simulations to maintain the needed proficiency of the team as a whole. A by-product of the operations training is a rigorous check of the procedures as well as an evaluation of the operator's skill level and proficiency. This provides operational feedback to the system to allow for an avaluation of proposed approachs for hazard control. Sometimes an alternate approach must be considered if the procedural method will not work, or perhaps some combination of the two will be used.

The Space Shuttle Mission Simulation System utilizes a copy of the flight software load as configured for the actual mission being trained for, as well as a high fidelity representation of the hardware directly utilized by the crew. Configuration of the simulation is maintained up-to-date with the real flight system, and therefore provides a realistic basis for evaluation of hazard controls involving the flight crew. during training the operations team is frequently exposed to real time situations requiring them to deal expertly with risk situations thereby maintaining a high level of awareness and competency.

At this point in the program, there are a variety of processes in place to provide the necessary management confidence that the Space Shuttle is acceptable to fly a given mission. Some of the processes are in place

primarily for the verification of configuration changes to systems and the flight software. Others are in place to support the training necessary to provide proficient personnel to conduct mission operations. Failure modes that have escaped previous analysis and testing are still occasionally being discovered through this process. Some of them are critical enough to cause the program management to make design changes. Therefore any major operations program must have a process to deal with the evaluation of risks throughout the life of the program.

WHAT IS NEEDED FOR THE NEXT PROGRAM

The Space Shuttle Program has evolved into a management process that has proven to be effective in dealing with a wide variety of complex risk scenarios. Potential risks when identified are dealt with in an efficient manner, and accountability for identification and resolution is established to allow this to happen. The program has a number of processes in place to surface potential risks as it evolves to its operational state. the fact that escapes from these processes are still occasionally discovered is an indication that improvements in the techniques and methodology for risk analysis would be of potential benefit to the program. This is especially true if these improvements were made early in the development phase when the leverage on cost is very high.

Basically, new analysis tools are needed that take advantage of the capabilities of modern ADP systems to be employed as an adjunct to the desing activity for both hardware and software. Many of the analysis techniqeus now in use are operator-dependent in that the results are directly relatable to the capabilities and knowledge of the operator. The technology now available is the development of expert systems for this application. By electronic

means, these systems could access engineering data bases containing the latest up-to-date configuration data for both hardware and software.

A system of this nature should be designed to meet the following objectives:

a. Be rigorous.

b. Provide repeatable results by any operator.

c. Provide a response in a timeframe to support the design activity.

d. Shift the drudge work to automation allowing the analyst more time for evaluation.

e. provide applications to cover software logic, electronic circuitry, mechanical systems, and operationsl procedures.

f. utilize available configuration data in a digital format.

g. Accommodate human intervention and analysis where needed.

h. Provide a capability to support real time operations as needed.

CONCLUSIONS

The Space Shuttle has established an effective risk managment structure to deal with the many complex risk issues facing operational manned space flight. It has functioned well as the Program progressed from its initial flight to its current near-operational state. As with any program, many of its features are shaped by compromises, the realities of available resources, and the engineering capability available at any point in time. The essential features of the Space Shuttle Risk Management approach are:

a. Responsibility and accountability at all levels of the program.

b. Structured review points throughout the development phase.

c. Product assurance organizations established to track and insure that the risk baseline is properly dealt with.

d. An effective mix of engineering analysis tools which provide the essential data for making informed risk decisions.

e. Continuity of involvement by the same management team charged with responsibility for making all the important management decisions.

f. Benefit of an effective independent systems engineering organization with an operations viewpoint.

g. An effective operator training system with a strong emphasis on dealing with potential risk scenarios.

h. A mandatory management review with high Agency visibility before each flight that addresses each new risk issue as well as the aggregate risk for that flight.

i. And finally a corporate culture oriented toward the elimination of risk situations for the program.

While the Space Shuttle Program has adopted a risk management appraoch that is adequate for meeting the needs of a major national operational program, ther are improvements in the analysis methodology that need to be addressed for new programs. These improvements will capitalize on current technology and provide substantive increases in productivity as well as better determination of potential hazards. This emphasis will increase our ability to eliminate many risks at an early stage of the design process - before changes become cost-prohibitive.